UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NESPRESSO USA, INC., Plaintiff, v. PEET'S COFFEE, INC., Defendant.	Case No. 1:22-cv-02209 (CM) (RWL)

~~[PROPOSED]~~ CASE MANAGEMENT ORDER REGARDING DOCUMENT AND ELECTRONICALLY STORED INFORMATION PRODUCTION PROTOCOL

1. Purpose

This Order will govern the production of Documents (as defined below) by Plaintiff Nespresso USA, Inc. and Defendant Peet's Coffee, Inc., (each a "Party" and collectively, the "Parties") in accordance with applicable provisions of the Federal Rules of Civil Procedure ("Federal Rules") and the Local Rules of the United States District Court for the Southern District of New York ("Local Rules"), in connection with the above-captioned matter (the "Action").

The production of Documents by the Parties also shall be subject to the provisions of any orders concerning confidentiality and privilege as agreed to among the Parties and/or entered by the Court ("Protective Order"), and nothing in this Order shall be interpreted to supersede the provisions of any such Protective Order.

Nothing in this Order shall be interpreted to compel disclosures of information or as a waiver by any Party of any objections to the discoverability, admissibility, or confidentiality of Documents or information contained therein.

2. Definitions

a. "Confidentiality Designation" means the legend affixed to Documents or ESI for confidential, highly confidential information, or highly confidential—outside counsel eyes only information as defined by, and subject to, the terms of the Protective Order.

b. "Document" is defined to be synonymous in meaning and equal in scope to the usage of this term in Rules 26 and 34 of the Federal Rules and Rule 26.3 of the Local Rules. The term "Document" shall include Hard-Copy Documents, Electronic Documents, and ESI as defined herein.

c. "Electronic Document or Data" means Documents or data existing in electronic form at the time of collection, including but not limited to: e-mail or other means of electronic communications, word processing files (e.g., Microsoft Word), computer slide presentations (e.g., PowerPoint or Keynote slides), spreadsheets (e.g., Excel), and image files (e.g., PDF).

d. "Electronically stored information" or "ESI," as used herein, has the same meaning as in Rules 26 and 34 of the Federal Rules, and includes Electronic Documents or Data, and computer-generated information or data, stored in or on any storage media located on computers, file servers, disks, tape, USB drives, or other real or virtualized devices or media in the Parties' possession, custody, or control.

e. "Extracted Full Text" means the full text that is extracted electronically from native electronic files, and includes all header, footer, and document body information.

f. "Hard-Copy Document" means documents existing in paper form at the time of collection.

g. "Hash Value" is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the

characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same Hash Value, no matter how similar they appear, is less than one in one billion.

h. "Load files" means an electronic file containing information identifying a set of paper-scanned images, processed ESI, or native format files, as well as the corresponding Extracted Full Text or OCR text files, and containing agreed-upon extracted or user-created metadata, as well as information indicating unitization (i.e., document breaks and document relationships such as those between an email and its attachments) used to load that production set into the document review platform of the Party receiving a production ("Receiving Party"), and correlate its data within that platform. A load file is used to import all image, native, and text files and their corresponding production information into a document database. The Producing Party shall produce a load file for all produced Documents with each particular production in accordance with specifications provided herein.

i. "Media" means an object or device, real or virtual, including but not limited to a disc, tape, computer, or other device on which data is or was stored.

j. "Metadata" means: (i) information embedded in or associated with a native file that describes the characteristics, origins, usage, and/or validity of the electronic file; (ii) information generated automatically by the operation of a computer or other information technology system when a native file is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system, (iii) information, such as Bates numbers, redaction status, or confidentiality status created during the course of processing Documents for production, and (iv) information collected during the course of collecting Documents, such as the name of the media device on which it was

stored, or the custodian or non-custodial data source from which it was collected. Nothing in this Order shall require any party to manually populate the value for any metadata field.

k. "Native Format" or "native file" means the format of ESI in which it was generated and/or used by the Party producing the Documents (the "Producing Party") in the usual course of its business and in its regularly conducted activities. For example, the native format of an Excel workbook is an .xls or .xlsx file.

l. "Optical Character Recognition" or "OCR" means the optical character recognition technology used to read the text within electronic images of Hard-Copy Documents and create a file containing a visible, searchable text format of such Documents.

m. "Searchable Text" means the native text extracted from an Electronic Document and any Optical Character Recognition text ("OCR text") generated from the electronic image of a Hard-Copy Document, an Electronic Document that has a native image format, or a redacted image of an Electronic Document.

3. Deduplication

a. To the extent exact duplicate Documents reside within a Party's ESI data set, the Party shall produce only a single, deduplicated copy of a responsive Document. "Exact duplicate" shall mean bit-for-bit identity of the Document content with exact hash value matches; so-called "near duplicates" will not be included within this definition.

b. To the extent a Party de-duplicates its Documents, it shall de-duplicate stand-alone Documents or entire Document families in their ESI sources by the use of MD5, SHA-1, or SHA256 hash values. Where any such Documents have attachments, hash values must be identical for both the Document plus-attachment (including associated metadata) as well as for any attachment (including associated metadata) standing alone.

c. A Producing Party shall de-duplicate Documents across custodians and populate a field of data that identifies all custodians who had a copy of the produced Document (the "All Custodians" field); such de-duplicated Documents shall be deemed produced from the custodial files of each such identified custodian for all purposes in this Action, including for use at deposition and trial. A Producing Party shall use a uniform description of a particular custodian across productions. Multiple custodians in the "All Custodians" field shall be separated by a semicolon. Entity/departmental custodians should be identified with a description of the entity or department to the extent applicable.

d. No Party shall identify and/or eliminate duplicates by manual review or some method other than by use of the technical comparison using MD5 or SHA-1 hash values outlined above.

e. Hard-Copy Documents shall not be eliminated as duplicates of ESI.

f. If the Producing Party makes supplemental productions following an initial production, that Party also shall provide with each supplemental production an overlay file to allow the Receiving Party to update the "All Custodians" field. The overlay file shall include all custodians listed in the "All Custodians" field in prior productions and any custodians newly identified in the current supplemental production.

4. Production Format and Processing Specifications

a. Standard Format. Unless otherwise specified in Section 4(b) or pursuant to Section 4(i) below, the Parties shall produce Documents in tagged image file format ("TIFF"). TIFFs of ESI shall convey the same information and image as the original Document, including all commenting, versioning, and formatting that is visible in any view of the Document in its native application. To the extent possible, the Producing Party will instruct its vendor to force off Auto

Date. Any TIFFs produced shall be single-page, 300 DPI, Group IV TIFF files. After initial production in image file format is complete, a Party must demonstrate particularized need for production of ESI in its native format. Notwithstanding the foregoing, should a Party determine that a particular Document or Documents requires color in order to be read or interpreted, the Parties shall work together in good faith to coordinate the production of such Documents in color as JPEG files.

b. Native Format. Except as provided by Section 4(i) below, the Parties shall produce all spreadsheets, computer slide presentations, audio files, video files, and other file types that cannot be accurately represented in TIFF format in native format, provided, however, that the Parties will meet and confer regarding appropriate format of production for databases and structured data (e.g., Microsoft Access, Oracle, or other proprietary databases). For each Document produced in native format, a responding Party shall also produce a corresponding cover page in TIFF image format, specifying that the Document has been "produced in native format" and endorsed with the Bates Number and Confidentiality Designation, if applicable, which will be inserted into the image population in place of the native file. Computer slide presentations (i.e., "PowerPoint" presentations) will be produced in native format. When the native file is produced, the Producing Party shall preserve the integrity of the Electronic Document's contents, i.e., its original formatting and metadata.

c. Embedded Objects. If Documents contain embedded objects, the Parties shall extract the embedded objects as separate Documents and treat them like attachments to the Document to the extent reasonably possible. To the extent reasonably possible, images or zero-byte files embedded in emails shall not be extracted and produced separately.

d. Load Files. Each production of Documents shall be accompanied by delimited load files (i.e., dat and/or .opt) containing a field with the full path and filename to files produced in native format and also containing metadata fields identified in Appendix A, to the extent the information is available in the original ESI file and can be extracted without unreasonable burden using standard litigation support processing platforms (except for vendor-generated fields related to the litigation production, such as "BegBates," "EndBates," bases for redaction, and Confidentiality Designations).

e. .Txt Files. For all Documents containing extracted full text or OCR text, the Producing Party shall provide searchable Document level .txt files (named using the Bates start/"BegBates"), which shall be included in the load file and the path to the text file provided in the metadata .dat file.

f. Bates Numbering and Other Unique Identifiers. Every item or file of ESI that is produced shall be identified by a unique page identifier ("Bates Number") and a Production Volume Number for any storage device (e.g., CD, USB, hard drive) containing such files. All Bates numbers will consist of an Alpha Prefix, followed by a numeric page index. There must be no spaces in any Bates number. Any numbers with less than 8 digits will be front padded with zeros to reach the required 8 digits. All ESI produced in TIFF format shall contain a unique Bates Number on each page of the Document, electronically "burned" onto the image at a location that does not obliterate, conceal, or interfere with any information from the source Document. If a member of a Document family that has otherwise been determined to be responsive cannot be technically processed (e.g., unsupported file format, file corruption, inaccessible password-protected Document), those technical problems shall be identified and disclosed to the Receiving Party by production of a Bates-labeled slip sheet that states "Technical issue—file cannot be

processed"; the associated metadata for the file with the technical problem shall be produced if technically possible. A Receiving Party thereafter may raise with the Producing Party any questions or concerns, and the Parties shall meet and confer to attempt to resolve any issues.

g. Hard-Copy Documents. Except as otherwise set forth in this paragraph, the Parties agree that responsive Hard-Copy Documents shall be converted to single-page TIFF files, and produced following the same protocols set forth in Section 4(a) above, including the production of OCR text that is generated to make such Documents searchable. Generally, all Hard-Copy Documents will be scanned and produced electronically, unless a Party establishes good cause for producing such Documents via Hard-Copy. In scanning all Hard-Copy Documents, Hard-Copy Documents should be unitized as they existed in the ordinary course. Accordingly, distinct Documents should not be merged into a single record, and single Documents should not be split into multiple records. In the case of an organized compilation of separate Documents (for example, a binder containing several separate Documents behind numbered tabs), each of the Hard-Copy Documents should be separately scanned, but the relationship among the Documents in the compilation should be reflected in the proper coding of the beginning and ending Documents and attachment fields. The Parties will make their best efforts to unitize the Documents correctly. Producing Hard-Copy Documents as provided herein does not change their character from Hard-Copy Documents into ESI. For Hard-Copy Documents, the Parties need only populate metadata fields for the beginning and end bates number, production volume, custodian, confidentiality designations (if applicable), redactions (if applicable), as well as information regarding attachments (if applicable).

h. Confidentiality Designation. To the extent any Document (or portion thereof) produced as a TIFF image in accordance with this Order is designated with any type of

confidentiality designation under the Protective Order, the Producing Party will brand the required Confidentiality Designation in a corner of any TIFF images representing the produced item and in a consistent font type and size that does not obscure any part of the underlying image or Bates number, to the extent possible.

i. Privilege. Pursuant to Federal Rule of Civil Procedure 26(b)(5)(A)(ii) and Local Rule 26.2 of the Southern District of New York, the Parties shall produce a log of all documents or information withheld on the grounds of the attorney-client privilege or work product doctrine. Notwithstanding the foregoing, the Parties agree that the following items, to the extent that they are privileged or constitute protected attorney work product, need not be included on a privilege log: (i) communications concerning this Action that are between a Party and outside legal counsel; (ii) attorney work product of the Parties' respective outside legal counsel and/or in-house legal counsel concerning this Action; (iii) communications concerning this Action (but not merely the subject matter at issue in the Action) that were both (a) exclusively between a Party and its in-house legal counsel or in-house legal counsel of an affiliate, and (b) made on or after January 1, 2022; and (iv) internal communications within a law firm retained by a Party as counsel for this Action. For purposes of this paragraph 4.i. only, the term "Action" shall also include the pending Opposition Proceeding before the Trademark Trial and Appeal Board, Opposition No. 91265038, between Peet's Coffee, Inc. and Société des Produits Nestlé S.A.

The Parties further acknowledge and agree that the Parties' privilege logs need not contain separate log entries for individual emails within an email chain, provided that the corresponding privilege log entries reasonably identify such individual emails.

j. Metadata or Categorical Privilege Logs. The Parties may employ metadata or categorical privilege logs, where appropriate. Any such metadata or categorical privilege log must

include at least the following information, for each withheld category: (i) date of documents withheld; (ii) file type of document type(s) withheld; (iii) identities of all sender(s), recipient(s) and copyee(s) on communications, to the extent such information may be automatically extracted using technological methods; (iv) file name, subject line, or categorical description sufficient to adequately describe the documents and to allow the opposing party to determine why the privilege might apply; (v) basis for withholding; and (vi) total number of documents withheld.

k. Redactions. A Party may redact from Documents information protected by the attorney-client privilege, work product privilege, or any other applicable privilege or immunity; to remove social security numbers, bank account information, and other personally identifiable sensitive information (e.g., customer surnames, phone numbers, email addresses, credit card information); and to comply with any applicable laws and regulations. Other than as expressly permitted by this Order or the Protective Order, no redactions may be made within a produced Document. For avoidance of doubt, the Parties may not withhold from production or redact non-privileged, substantive portions of responsive documents on the basis of non-relevance.

Any redactions shall be clearly indicated on the face of the Document, with each redacted portion of the Document stating that it has been redacted, and a metadata field shall indicate that the Document contains redactions. Where a responsive Document contains both redacted and non-redacted content, the Producing Party shall produce the remainder of the non-redacted portions of the Document and the text/OCR corresponding to the non-redacted portions.

Email header information should not be redacted unless it is independently privileged. The production of a Document in a redacted form does not affect the Producing Party's obligation to timely assert and substantiate the assertion of privilege over the content in a privilege log. The

Parties shall honor reasonable requests for the production of particular redacted Documents in other formats where the TIFF image is not reasonably usable.

l. Parent-Child Relationships. Parent-child relationships within a Document family (the association between an attachment and its parent Document or between embedded Documents and their parent) shall be preserved. Responsive non-privileged Electronic Documents attached to an email or embedded within other Electronic Documents and Hard-Copy Documents attached or appended to Hard-Copy Documents must be mapped to their parent by the beginning Bates number and immediately follow that parent file in the sequence of the production. Email attachments and embedded files or links "BegRange" and "EndRange" fields listing the unique beginning Bates number of the parent Documents and ending number of the last attachment must be populated for each child and parent Document.

m. OCR. OCR software shall be set to the highest quality setting during processing.

n. Deviation from Production Specifications. If a particular Document or category of Documents warrant a different format, the Parties will cooperate in good faith to arrange for a mutually acceptable production format.

o. Password Protection. In the event any Document (or portion thereof) produced is password protected, the Producing Party shall provide access to the data or the password needed to access the Document, except where a password is unknown to or inaccessible by the Producing Party following a good faith effort to secure or determine such password.

p. Use at Deposition. Any Document produced in native format that a party identifies and/or marks as an exhibit at a deposition must include as part of that identification or exhibit the produced corresponding cover page in TIFF image format, endorsed with Document's Bates Number and Confidentiality Designation, as described in Section 4(a), above.

q. Tracked Changes and Comments. To the extent that a document contains tracked changes or comments, the document should be imaged showing any such tracked changes and/or comments or produced in native form.

5. Production Media

The Producing Party shall produce Documents on readily accessible, computer or electronic media, including CD-ROM, DVD, external hard drive (with standard PC compatible interface), via secure FTP site, or such other readily accessible computer or electronic media as the Parties may agree (the "Production Media"). Each piece of Production Media shall be encrypted and assigned a production number or other unique identifying label ("Production Volume Number"), and shall include (a) the name of the Action and the Civil Action Number; (b) the identity of the Producing Party; (c) the production date; (d) the Bates Number range of the materials contained on such Production Media item; and (e) the Production Volume Number of the Production Media. The Producing Party shall accompany all Document productions with a transmittal cover letter identifying by Bates number the Documents produced. If the Producing Party produces Documents via secure FTP site, the materials will remain available via the secure FTP site for no fewer than fourteen (14) days from the date of production, and the Producing Party shall, within a reasonable time, accommodate requests from the other Party that Documents be reposted to the FTP site.

6. Cost Shifting

The costs of production pursuant to this Order shall be borne by the Producing Party. However, in agreeing to this Order, no Party waives or relinquishes any right or interest it may have under the Rules of Civil Procedure to seek cost shifting or apportionment for the costs of electronic discovery.

7. Third-Party ESI

a. A Party that issues a non-party subpoena (the "Issuing Party") shall include a copy of this Order and the Protective Order with the subpoena and state that the Parties in the Action have requested that third parties produce Documents in accordance with the specifications set forth herein.

b. The Issuing Party shall produce to the other Party any Documents (including any metadata) obtained under any subpoena to a non-party within twenty days from receipt of the Documents by the Issuing Party.

c. If the non-party production is not Bates-stamped, the Issuing Party shall promptly inform the other Party, and the Parties shall meet-and-confer in good faith to discuss (i) whether unique Bates prefixes and numbering schemes should be added, and (ii) if so, a reasonable and cost-effective approach for doing so.

8. Best Efforts Compliance and Disputes

The Parties agree to use their best efforts to comply with and resolve any differences concerning compliance with any provision/s of this Order. If a Producing Party cannot comply in a particular circumstance with this Order, such Party shall promptly inform the Receiving Party in writing why compliance with the Order is not reasonable or feasible. No Party may seek relief from the Court concerning compliance or non-compliance with the Order until it has met and conferred with the other Party in a good faith effort to resolve or narrow the area of disagreement.

9. Modification

This Order may be modified by a Stipulated Order of the Parties or by the Court for good cause shown.

SO ORDERED:

10/11/2022

HON. ROBERT W. LEHRBURGER
UNITED STATES MAGISTRATE JUDGE

Appendix A

Beginning Bates (BegBates)

End Bates (EndBates)

Begin Attachment

End Attachment

Path

Create date

Create Time

Last Modified Date

Last Modified Time

Date Sent

Time Sent

Date Last Printed

Time Last Printed

Saved By

Date Last Saved

Time Last Saved

Date Received

Time Received

File Type

Document Title

Email Subject

Custodian

All Custodians

Author

From

To

CC

BCC

E-mail Sensitivity

File Extension

File Name

Confidentiality (Confidential)

Redaction Type

MD5 Hash